Microsoft

DEVELOPING A CITY STRATEGY FOR CYBERSECURITY

A seven-step
guide for local
governments

CRISTIN FLYNN GOODWIN
J. PAUL NICHOLAS

October 2014

Contents

Introduction 3

The evolving world of connected cities 4

Principles of a cybersecurity strategy 5

Understanding the threat landscape in cyberspace 5

Laying the groundwork for developing a cybersecurity strategy 7

Creating a strategy for city cybersecurity 9

- Build a risk-based approach to cybersecurity 10
- Set clear priorities 12
- Define minimum ICT security baselines 13
- Share and coordinate threat and vulnerability information 14
- Build incident response capabilities 16
- Boost public awareness, education, and workforce training 18
- Enable public, private, and academic cooperation 19

Conclusion 21

Cybersecurity strategy checklist 22

Introduction

Cities today are vibrant centers of modern life and modern economies, which increasingly depend on information and communications technology (ICT). Along with the growing economic value of ICT for cities, threats to it grow apace. In this security environment, a strategy to protect a city's cybersecurity is critical for managing risks and boosting resilience. A secure city can be confident that it is better positioned for opportunity and growth.

On a national level, policymakers are grappling with principles, laws, policies, and programs to improve cybersecurity. Cities are now becoming a crucial part of this discussion because they, too, are the targets of cyberattacks. Cities have practical security needs that cannot wait for international and national politics to keep pace. They need immediate ways to prioritize risks and to assign roles and responsibilities for key aspects of cybersecurity. Cities also have to balance costs, existing and legacy systems, and administration of new programs and systems. A local cybersecurity strategy can help a city get started.

Microsoft has years of experience dealing with threats in cyberspace around the world. For example, each month, the company receives threat information from more than 600 million systems in more than 100 countries and regions. Leveraging this vast knowledge of threats, along with the company's long experience working with governments on finding solutions to cybersecurity challenges, Microsoft has created a principled seven-step approach to help cities design and implement cybersecurity strategies that fit within other transformational urban programs aimed at increasing resilience:

1. Build a risk-based approach to cybersecurity
2. Set clear priorities
3. Define minimum ICT security baselines
4. Share and coordinate threat and vulnerability information
5. Build incident response capabilities
6. Boost public awareness, education, and workforce training
7. Enable public, private, and academic cooperation

The evolving world of connected cities

Every region of the world is experiencing rapid urbanization. Today, more than half of the world's population lives in urban areas, and by 2050, that number will grow to nearly 70 percent, or more than 6 billion people.[1] Although some areas will experience greater urbanization than others (for example, India will almost double its urban population between 2011 and 2031[2]), dramatic urban growth has become a truly global phenomenon.

As a city leader, managing this extraordinary rate of growth can be difficult. City resources are stretched, planning is hampered by economic realities, and the critical challenges of today, such as aging infrastructures, require significant attention.

Amplifying the challenges of rapid urbanization is the Internet of Things, a term which defines a web of interconnected people, devices, and systems. By 2020, more than 50 billion objects are expected to be connected to the Internet.[3] Furthermore, a recent study conducted for Microsoft[4] predicts that there will be 4.7 billion Internet users in 2025, with nearly half coming online between 2012 and 2025—almost entirely from emerging economies. Many of these connections will come from mobile broadband devices, such as phones and tablets. However, with increasing connectivity comes increased risk to city data, systems, and infrastructure.

Resilience

Resiliency has become important for cities as the physical, social, and economic challenges of the 21st century manifest themselves in urban environments. Indeed, as cities become more interconnected, cybersecurity plays a crucial role in resilience efforts.

Today's cyberenvironment poses significant risks to a city if not managed purposefully. The following factors play a role in boosting resilience:

Expanded Internet access for citizens. Increased Internet connectivity supports a city's resilience by providing paths for communication, increasing education, and stimulating economic growth. According to the International Telecommunications Union (ITU), 78 percent of homes in developed countries have Internet access, and mobile-broadband penetration is at 84 percent. Developing countries will see the most mobile growth in 2014, with 55 percent of all mobile-broadband subscriptions.[5]

Use of smart technology. Cities have been successful in using smart technology, such as big data analytics and mobile applications, to improve citizen services. During the 2012 Summer Olympics, the City of London improved its transportation system by making more of its data available to citizens. Information about service disruptions and real-time bus arrival times was offered through smartphone apps, allowing people to safely and efficiently navigate the city.

Gathering and sharing information. Information-gathering and sharing helps increase innovation and decrease security threats. Creating a cybersecurity dashboard, such as the one developed by Microsoft partner, Swan Island Networks,[6] is one way that cyberthreat information can be gathered and shared. This customizable dashboard consolidates hundreds of data sources to provide cities with a real-time picture of current threats, along with alerts that make the information actionable.

Benefits of the cloud

With its flexible, scalable architecture, cloud computing helps boost a city's efficiency and quality of service, while supporting participation in the global economy.

The cloud can help cities:

- **Boost resiliency.** With centralized data storage, management, and backups, data recovery in response to local disruptions can be faster and easier.
- **Increase efficiency.** Cloud services can be adjusted, as needed, to improve operational efficiencies.
- **Simplify operations.** The cloud can help streamline facilities and reduce ICT management requirements.
- **Provide better citizen services.** Innovative new services are now possible with data in the cloud and with applications in the hands of citizens.

[1] World Urbanization Prospects: The 2014 Revision. United Nations, Department of Economic and Social Affairs, Population Division. 2014. http://esa.un.org/unpd/wup/Highlights/WUP2014-Highlights.pdf

[2] Building and managing intelligent cities in India. Accenture. December 17, 2013. http://timesofindia.indiatimes.com/tech/tech-news/software-services/Proud-that-Indias-a-source-of-global-tech-talent-Satya-Nadella/articleshow/31750255.cms

[3] Evans, Dave. "The Internet of Things: How the Next Evolution of the Internet is Changing Everything." Cisco. April 2011 http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[4] Burt, David, Aaron Kleiner, J. Paul Nicholas, and Kevin Sullivan. Microsoft Cyberspace 2025. Microsoft. June 2014. http://download.microsoft.com/download/C/7/7/C7775937-748E-4E95-85FB-24581F16B588/Cyberspace%20 2025%20Today's%20Decisions,%20Tomorrow's%20Terrain.pdf

[5] "ITU releases 2014 ICT figures." ITU. May 5, 2014. http://www.itu.int/net/pressoffice/press_releases/2014/23.aspx#.U4feMKxOXbg

[6] "TIES for Microsoft CityNext: Cyber Edition." Swan Island Networks. http://swanisland.net/products/city/cyber-edition

Principles of a cybersecurity strategy

A cybersecurity strategy should have a clear set of principles to help frame decisions on identifying, managing, and mitigating cybersecurity risks in a way that balances civil rights and privacy, costs, and other priorities in today's push toward cloud- and mobile-connected cities. Microsoft recommends these principles to guide a city's cybersecurity strategy:

Cybersecurity principles	**Risk-based.** Assess risk by identifying threats, vulnerabilities, and consequences, and then manage it through mitigations, controls, costs, and other measures.
	Outcome-focused. Focus on the desired end state rather than prescribing the means to achieve it, and measure progress toward that end state.
	Prioritized. Adopt a graduated approach to priorities, recognizing that disruption and failure are not equal among critical assets or across critical sectors.
	Practicable. Optimize for adoption by the largest possible group of critical assets and for implementation across the broadest range of critical sectors.
	Respectful of privacy and civil liberties. Include protections based upon the Fair Information Practice Principles and other internationally accepted privacy and civil liberties policies, practices, and frameworks.
	Nationally and globally influenced. Integrate national and international standards to the maximum extent possible, keeping harmonization in mind.

What is cybersecurity?

For a city, cybersecurity is the protection of data, systems, and infrastructure vital to the city's operation and to the stability and the livelihood of its people.

Understanding the threat landscape in cyberspace

Prior to developing a cybersecurity strategy, a city should examine its threat landscape. The types of online threats facing city data, systems, and infrastructure have grown more complex and include everything from malicious software and spam to online fraud and terrorist activity.

Data. The flow of information is critical to a city's ability to maintain services and to connect with citizens. Health records, police reports, and business taxes all contain data that must be protected. Although use of smart data is vital to improving public services, it also means that there is an increasing amount of personally identifiable information (PII) at risk.

Data threats are primarily manmade, although loss of data due to natural disaster (like a flood, tsunami, or hurricane) can occur. Such threats may be not be malicious, such as the unintentional download of infected software. For example, when a technician unknowingly inserted an infected USB drive into a network computer, the resulting virus attack downed a turbine control system at a US power company for three weeks.[7]

[7] Finkle, Jim. "Malicious virus shuttered power plant: DHS." Reuters. January 16, 2013. http://www.reuters.com/article/2013/01/16/us-cybersecurity-powerplants-idUSBRE90F1F720130116

Online threats

Hackers and other criminals are accelerating their attacks on computers around the world, with:

- Malicious software and spam.
- Phishing tactics.
- Scams and online fraud.
- Distributed-denial-of-service (DDoS) attacks.
- Botnets.
- Software piracy, copyright infringement, and trademark violations.

However, threats are more likely to be malicious, such as an insider stealing or corrupting data, or a hacker installing a botnet or disrupting services with a DDoS attack. Two recent incidents illustrate the vulnerabilities of municipal data. In late 2013, a flash drive was stolen from a Milwaukee contractor in the United States. The drive contained the unencrypted Social Security numbers and personal information of 6,000 city employees.[8] Furthermore, the city of Johannesburg, South Africa, experienced a breach of its IT system, exposing customer rates and service invoices to potential fraud.[9]

Systems. A city's digital systems are vital to its continued operations. School systems use online tools to facilitate learning and to record and track student performance. Online systems for law enforcement help ensure that citizens are safe and protected. Emergency communications systems are crucial during storms or medical emergencies. The compromise of any of these can interrupt city services and put citizens at risk. As with threats to data, systems may be compromised by both malicious and unintentional actions.

Infrastructure. Many major cities own, operate, or regulate critical infrastructure, such as electrical grids, water delivery systems, and transportation. More and more, these key public utilities are being transitioned to systems that rely on ICT to improve efficiency, but the increased connectivity and the wide use of third-party contractors heighten infrastructure vulnerability to cyberattack. The US Department of Homeland Security said that the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 198 incidents reported by energy companies, public water districts, and other infrastructure facilities in the fiscal year ending September 30, 2012.[10] Typhoon Haiyan in Southeast Asia caused major infrastructure devastation—power and communications systems were disabled, in some areas, for months. Additionally, some experts blame cyberattacks for the northeast blackout of 2003, the largest blackout in North American history, which affected 50 million people in a 9,300-square-mile area, and for the massive 2008 Florida blackout that shut down large portions of the power grid.[11]

Learning from Tallinn, Estonia

In the spring of 2007, computer systems and networks in Estonia were subjected to a massive DDoS attack which emanated from abroad. Government services, such as the Ministry of Defense email network, in addition to private services, like bank websites and ATM networks, were disabled, rendering most public or private business effectively incapacitated during the roughly 48 hours of the attack. No physical damage occurred. Nevertheless, the attack intermittently paralyzed financial and government activity in the country for a few weeks.

The Estonian government and private sector used the incident to learn how to better protect their operations. As a result, Estonia has fortified electronic signatures, firewalls, and backup systems, and it has become a champion of cybersecurity.

[8] "Notice of Privacy Incident." United/Dynacare, LLC. 2013. https://www.dynacaremilwaukee.com/Downloads/Dynacare%20SubNotice%20Rev112013.pdf

[9] "Breach of Our IT System." City of Johannesburg. August 22, 2013. http://www.joburg.org.za/index.php?option=com_content&id=8771:22-08-2013-breach-of-our-it-system

[10] "ICS-CERT Monitor." U.S. Department of Homeland Security. https://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monitor_April-June2013.pdf

[11] Harris, Shane. "China's Cyber-Militia." National Journal. May 31, 2008. www.nationaljournal.com/magazine/china-s-cyber-militia-20080531

Laying the groundwork for developing a cybersecurity strategy

Another important step for a city to take before starting a cybersecurity strategy is to research national and regional requirements regarding cybersecurity. In addition, cities should examine the preparedness of internal organizations and then address how to fund their strategies.

Research requirements and regulations

Today, most national governments provide only voluntary guidance related to cybersecurity, but some are beginning to mandate compliance, particularly when it comes to critical infrastructures. Cities should therefore watch these developments closely. In Japan, a new bill would require all government ministries and agencies to report cyberattacks, giving the prime minister the authority to order them to comply.[12] Similar legislative requirements are being contemplated for critical infrastructure owners and operators in other parts of the world, such as in the European Union. In some cases, these requirements could apply to city-owned and -managed critical infrastructures.

Assess the readiness of the organizational and IT environment to support a cybersecurity strategy

Can the city's information technology (IT) architecture adequately address the complexity that arises from the development of a cybersecurity strategy? Does the strategy align with city needs? Does it adhere to required standards?

To ease deployment and communication, it helps to develop a clear map of all agencies and departments impacted by the cybersecurity strategy. This should include a determination as to whether agencies and departments have written information security plans and policies in place and as to how often they exercise or test the plans.

Additionally, reviewing findings of security audits can help a city better understand the efficiency and effectiveness of the management, technical, and operational security controls that are needed to implement the cybersecurity strategy.

[12] Mie, Ayako. "New cybersecurity bill would order all ministries to report attacks." Japan Times. May 7, 2014. www.japantimes.co.jp/news/2014/05/07/national/new-cybersecurity-bill-require-ministries-report-attacks/#.U4fDqqxOXbgimpact-cybercrime2.pdf

The likely cost to the global economy from cybercrime was

$400B annualy.[13]

Secure funding

For most cities, balancing cybersecurity with other budget priorities will be a challenge, albeit one that can be lessened by understanding the return on investment from cybersecurity measures. In 2014, the Center for Strategic and International Studies produced Net Losses: Estimating the Cost of Cybercrime; Economic Impact of Cybercrime II, which estimated that the likely cost to the global economy from cybercrime was $400 billion annually—or .8 percent of the estimated global GDP.[14] To assess the return on investment for cybersecurity measures, a city should consider the economic impact of cyberattack on citizens, law enforcement, local businesses, and city administration.

City leaders need to make cybersecurity a priority and then look for operational efficiencies. Some cities create champions, local government leaders who sponsor legislation and otherwise encourage funding. Education can also play an important role in convincing city funding authorities about the critical need for cybersecurity and how it fits into the city's overall approach to security. Or there may be a national grant system for particular high-threat, high-density urban areas.

Even without a large cybersecurity budget, cities can create an overall IT budget review process which retires old systems and which ensures that the procurement process for new products and services keeps top-tier security risks front of mind. The process should also reduce administrative costs, create flexibility, and increase security. Furthermore, many cities are turning to cloud computing to gain efficiencies in administration and operations and to improve security.

[13] *Net Losses: Estimating the Cost of Cybercrime; Economic impact of cybercrime II*. Center for Strategic and International Studies. June 2014. www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Creating a strategy for city cybersecurity

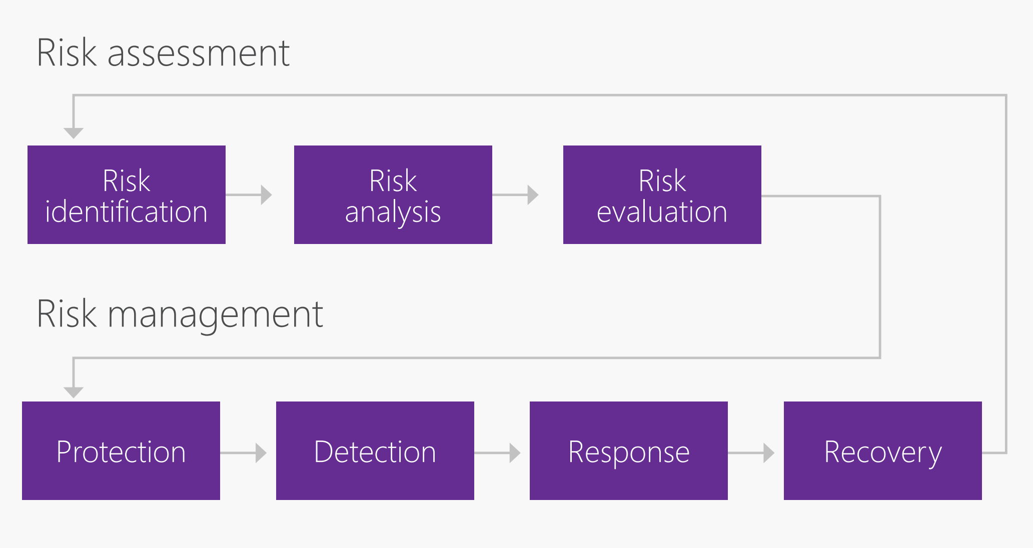
1 Build a risk-based approach to cybersecurity

The first step in developing a cybersecurity strategy focuses on identifying, analyzing, and evaluating the risks to be managed. Risks in cyberspace are typically thought of as risks to information systems, which, if exploited, could negatively impact the city's economic well-being or the public safety of its citizens to a significant degree.

A risk-based approach must look at the overall structure of a city's systems to determine where critical dependencies occur and to ascertain how to mitigate vulnerabilities to reduce the likelihood of system failure. City leaders should also consider leveraging tabletop exercises and technical reviews to understand interdependencies and single points of failure.

Recommendations

- **Develop a clear structure for assessing and managing risk.** It is helpful to use the following taxonomy:



- **Assess threats to the city's cybersecurity using threat modeling.** Threat modeling can help identify the assets a city is trying to protect, in addition to what it is protecting those assets from. A threat model inventories key municipal assets and the threats to them, determines the likelihood that assets will need protection, looks at a city's capability to defend against the threats, and determines the consequences of inaction. This approach allows city leaders to identify and mitigate potential security issues early, while the issues are still relatively easy and cost-effective to resolve. Categorizing online threats (as shown in the following table) can make it easier to assess threats and to then develop specific preventive and reactive strategies.

Threat	Examples	
Passive	Unintentional actions	Exposure to malware through email or websites
		Receipt of spam email or phishing
	Under-resourcing	Unprotected systems
		Unclear mitigation strategies
		Undefined response capabilities
		Lack of clear ownership
Active	Cybercrime	Fraud
		Distributed Denial of Service
		Theft of intellectual property or finances
		Abuse or damage of ICT systems
		Damage to critical infrastructure
	Natural hazards	Typhoons and hurricanes
		Earthquakes and tsunamis
		Floods
		Tsunamis
		Accidental cutting of undersea Internet cables

- **Document and review risk acceptance and exceptions.** When implementing a risk-based cybersecurity strategy, city leaders often find that, for the government to deliver services, some risks simply need to be accepted. It is impossible to mitigate every risk, and a framework for risk should include clear guidelines governing both how risks are accepted and when an asset is so vital that it must be protected. The risks being accepted and any relevant exceptions should be approved by the head of the responsible agency; in some instances, those risks should be taken to city leadership for approval.

  Within the cybersecurity strategy, city leaders should assign responsibility for accepted risks to pertinent personnel and should develop appropriate incident response plans to manage these risks. Registries of accepted risks should be reviewed on a regular basis to ensure that critical systems, whether government-owned or private, are not needlessly exposed.

- **Make citywide assessment and management of risk an ongoing process.** Risk assessment and risk management should be a continual process, not an end state. As technology evolves and as threats grow more sophisticated, there must be ongoing evaluations to assess whether current controls remain sufficient. Additionally, technologies may become available that allow for effective mitigation of previously accepted risks.

More information on building a risk-based approach to cybersecurity

- Local Government Cyber Security: Risk Management, A Non-Technical Guide: http://msisac.cisecurity.org/members/local-government/documents/Cyber-Security-Risk-Management-for-Local-Governments.pdf

- ISO Standard 31000:2009 Risk management—Principles and guidelines: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en

- National Institute of Standards and Technology (NIST) Guide for Conducting Risk Assessments: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=912091

2 Set clear priorities

Every city relies on certain critical services and functions or manages sensitive information which, if compromised, damaged, or destroyed through a cybersecurity incident, would dramatically impact the city's ability to function. The challenge of prioritization which systems to protect involves difficult trade-offs.

Although it is tempting to identify all municipal assets as high priority, it is critical to have a clear prioritization process. City leaders must review the strategy's principles and align priorities accordingly. It is important to define and implement a clear framework for classifying systems and data as high, medium, or low impact and to then use this to evaluate key city systems, even those operated by third parties. In addition, to ensure a common approach across the city enterprise, cities should map protection profiles to the classification of systems and data.

One of the best ways to prioritize risks is to use existing standards, however, risks often evolve too fast to be addressed by formal standards bodies. Additional risk management activities, such as a "top 20 critical security controls" approach advocated by organizations like SANS,[14] may augment standards to help in prioritization.

In February 2014, the US National Institute of Standards and Technology released a voluntary framework that includes standards, guidelines, and practices which can be used by cities to manage cybersecurity-related risk. Although it was published in the United States, the framework leverages work done around the world and can be applied to most cities. Another resource is "Critical Security Controls," which offer tangible methods to address risks to enterprise data and systems.

Recommendations

- **Educate city leaders to understand and support the principles and to manage priorities.** Educate city leaders to understand and support the principles and to manage priorities. It can be difficult to weigh trade-offs when setting priorities. Regular education of city leaders on cybersecurity principles makes it easier to negotiate priorities. Not all city leaders have a background in cybersecurity, but they can all engage in the process of setting priorities and of understanding how decisions impact city assets.
- **Consider resiliency.** A city's infrastructure is of little value if it is not consistently available. A city's strategy should prioritize resources, standards, and organizational support to ensure that the most essential city services have a higher level of resiliency than less critical services. For example, migrating to a cloud-based service is one way to provide additional bandwidth and capacity to ensure that a service remains operational during a crisis.
- **Leverage procurement processes to reflect priorities and risks.** Cities must ensure that its priorities are reflected in IT procurement. They can use the procurement process to learn about new technologies or capabilities that may help increase a city's cybersecurity and can help refine the way in which the city thinks about its technology lifecycle.

More information on setting cybersecurity priorities

- NIST Framework for Improving Critical Infrastructure Cybersecurity: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf
- SANS Institute Critical Security Controls for Effective CyberDefense: www.sans.org/critical-security-controls

[14] "Critical Security Controls for Effective CyberDefense." SANS Institute. www.sans.org/critical-security-controls

3 Define minimum ICT security baselines

A minimum security baseline is a minimally acceptable security standard (or best practice) which is designed to ensure that city departments have implemented basic security measures to reduce the risk of unauthorized access to IT resources and data. Security practices could include protocols for security patches, disabling unnecessary services, or desktop hygiene standards.

A report published by Verizon found that **97%** of investigated network breach incidents in 2012 **could have been prevented** by using simple or intermediate security controls.[15]

Recommendations

- **Establish minimum security baselines.** By setting baselines, a city assesses the existing ICT security practices of its departments and establishes minimum standards for the ICT security of government data, systems, and infrastructure.

  But a baseline is just that—a starting place from which city leaders should continue to drive security enhancements. As cities regularly improve security procedures, baselines must be reevaluated. There are a number of areas to apply baselines, including city systems, indirect systems (transit, water, education, and healthcare), city suppliers, and citizen cybersecurity.

- **Define clear roles and responsibilities for supporting a security baseline.** If there is no central agency responsible for ICT security, the cybersecurity strategy should recommend the establishment of an agency with appropriately skilled staff, along with adequate authority and resources to develop an ICT security baseline.

- **Establish a system for continuous security monitoring.** In an environment where threats are changing constantly, a city's cybersecurity strategy should recognize the need for continuously monitoring the security of systems, data, and infrastructure, rather than focusing on audits and paper-based compliance checks. Continuous monitoring automates the collection and analysis of data from a variety of sources to maintain an accurate description of an organization's security posture. Appropriate monitoring capabilities can make data available to determine whether a compromise has occurred, and these capabilities can support risk-management decisions.

There are standards, such as the security and privacy controls set by the NIST in Publication 800-53, which address continuous monitoring, dividing monitoring services into four categories:

- Baseline security monitoring for broad detection of malicious or anomalous network activity
- Specialized security monitoring for critical assets and processes
- Data analysis and reporting to provide telemetry to key internal security detection and response partners
- Policy enforcement and measurement of control effectiveness

More information on establishing ICT security baselines

- NIST Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication 800-53 (revision 4): nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- Council on Cybersecurity's Critical Security Controls for Effective CyberDefense: https://ccsfiles.blob.core.windows.net/web-site/file/c9665df3a5f54d2b8e6edab493c3b076/CSC-MASTER-VER50-2-27-2014.pdf
- NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

[15] Verizon RISK Team. 2012 Data Breach Investigations Report. March 22, 2012. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

4 Share and coordinate threat and vulnerability information

In the past year,

50%

of online adults

were cybercrime victims.[16]

Threats to and vulnerabilities in ICT systems are the currency of those who exploit city assets—and of those who would attack. In an ever-evolving threat environment, security responders need up-to-the-minute information about threats or vulnerabilities to protect these assets. Information about threats needs to be shared as quickly as possible to the widest audience so that threat actors can be stopped with minimal damage. A city's cybersecurity strategy should develop criteria for when and how this information is shared.

This can also help lead to new protections or mitigations, sometimes even before any negative impact. If done widely and efficiently, threat-sharing removes the head start afforded to an early attacker and prevents exploitation of security vulnerabilities, either by outside groups or from within. A cybersecurity strategy can help build a collaborative model in which information is shared, and those who are best positioned to act on it can do so.

Sharing information on threats is only the first step. There must be additional actionable steps that city agencies and citizens can take after vulnerabilities are exposed. The discovery in April 2014 of the Heartbleed security bug in OpenSSL, which enabled the theft of the private keys of approximately half a million of the Internet's secure web servers and which rendered users' session cookies and passwords vulnerable to hackers,[17] sheds light on the issue of when and how governments share information.

Recommendations

- **Set expectations for sharing threat and vulnerability information.** Everyone benefits when cities partner with national entities and the private sector to quickly share information about new threats and vulnerabilities. A city's cybersecurity strategy should recommend a clear communication path among city, regional, and federal governments and with the private sector.
- **Create a cross-city mechanism for sharing.** A city's strategy should include mechanisms for sharing information about incidents and indications of compromise. Cities should share this threat information within their agencies to better manage risk and to encourage cooperation and learning among city ICT professionals. Additionally, cities may want to share information with critical industry and infrastructure owners and with companies that have the ability to develop and disseminate updates to their customers. Having the right legal and technical frameworks in place to enable sharing helps to ensure a more effective response process and helps parties to stay focused on essential threats. This open sharing of information promotes stronger partnerships with the private sector and helps ensure that everyone is focused on critical threats.
- **Run cyberdrills to test game plans.** Drills with real scenarios should include all the members of a city's online incident response team—personnel from city, state, and federal agencies, in addition to participants from the private sector. Cities can also provide resources to help local businesses run their own drills, such as those run by the City of San Diego in partnership with the Naval Postgraduate School.[18]
- **Emphasize privacy and civil liberty protections in threat information-sharing.** There have been many discussions about the appropriate level of information that can and should be shared between private sector entities responding to vulnerabilities or threats and between those private sector entities and municipal agencies. It is important that a city strategy emphasize that, regardless of the scenario or type of data shared, steps are in place to ensure

[16] Warnick, Jennifer. "Microsoft, Digital Detectives." 2014. http://www.microsoft.com/en-us/news/stories/cybercrime/index.html

[17] "The Heartbleed Bug." Codenomicon. http://heartbleed.com/

[18] Dodd, David. "Channel Your Inner Hacker and Other Cyber Security Suggestions." Forbes. October 11, 2013. www.forbes.com/sites/xerox/2013/10/11/channel-your-inner-hacker-and-other-cyber-security-suggestions/

that privacy is always taken into consideration. In addition, ensuring adequate judicial oversight and enforcement of privacy protections is essential. Practices that govern sharing threat and vulnerability information must also uphold existing privacy laws in the city and the country, and even internationally, since information may be shared across borders.

➔ **Apply relevant national or international standards for information-sharing.** The concepts of encouraging common approaches to assessing and managing threats and vulnerabilities and of sharing information about them should be incorporated into a city's cybersecurity strategy.

For example, cities can use the ISO/International Electrotechnical Commission (ISO/IEC) standards on vulnerability handling within an enterprise (ISO/IEC 30111) and on vulnerability disclosure external to an enterprise (ISO/IEC 29147). These standards greatly improve the ability to handle complicated issues related to response. Also, encouraging greater use of Common Vulnerabilities and Exposures identifiers, and of taking steps to assess the severity and exploitability of a vulnerability, can increase capacity and readiness for complex response events. There are also machine-to-machine information-sharing standards, such as the Structured Threat Information eXpression (STIX) and the Trusted Automated eXchange of Indicator Information (TAXII) to represent structured threat information.

More information on sharing and coordinating threat and vulnerability information

- ISO/IEC 30111:2013: Information technology—Security techniques—Vulnerability handling processes: https://www.iso.org/obp/ui/#iso:std:iso-iec:30111:ed-1:v1:en
- ISO/IEC 29147:2014: Information technology—Security techniques—Vulnerability disclosure: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45170
- NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

5 Build incident response capabilities

The response to online threats requires sufficient capabilities to protect a city's people, information, systems, and infrastructure. A city's cybersecurity strategy should, therefore, clearly delineate what constitutes an incident which requires city involvement and triggers incident response plans and procedures, and what constitutes one which is the responsibility of the private sector, with a communication plan that bridges the two.

As indicated earlier, threats should be prioritized and a hierarchy of threats and associated responses, structured based on the anticipated impact, should be developed. It is important for cities to recognize that a threat to critical infrastructure systems, such as water or power, requires a significantly different response than does a threat to an isolated set of data or systems.

Integrating incident response into a city's existing incident command structure is another critical element of the strategy. In most cities, law enforcement and emergency services can provide established resources and personnel for an online response. A city's police department may include cyberforensics staff who can help identify, triage, and thwart online threats.

Fusion centers, information-sharing centers originally developed in the early 2000s under the US Department of Homeland Security, offer a good model for integrating existing incident response capabilities with cybersecurity. These centers empower front-line law enforcement, public safety, fire service, emergency response, public health, critical infrastructure protection, and private sector security personnel to gather, analyze, and share threat-related information.

Los Angeles Cyber Intrusion Command Center

Operated by the Los Angeles Police Department, with members from city and federal agencies, this 24-hour operations center monitors online threats against the city, and members meet regularly to discuss common threats and possible methods of neutralizing them.

Recommendations

- **Create a Computer Emergency Response Team (CERT).** Local governments, private companies, and universities can join together to develop CERTs to coordinate responses to computer security incidents. For help in constituting a municipal CERT, the global Forum of Incident Response and Security Teams is an excellent resource.[19]
- **Create clear ownership.** A cybersecurity strategy should recommend that the CERT lead any coordination between public and private sectors responding to online security incidents. The strategy should task the CERT with the technical and managerial duties to effectively assist government and critical private actors during crisis situations.
- **Engage private sector and national resources.** City agencies should work with the private sector to respond to online incidents. This includes clear communication paths for sharing information about threats and vulnerabilities, resources, and training. For example, the City of London Police developed a program with the British Bankers Association to train thousands of bankers each year to identify and respond to cybercrime and fraud in the financial sector. The program plans to provide workshops for banks around the world on threat identification and mitigation.
- **Enable consistent incident classification.** When delineating incident responses, cities must clearly distinguish between those incidents which require a city response and those which do not rise to that level. Because privately owned critical information and systems are likely targets for cyberattack, the city must be sure that those operators have a clear understanding of the role of government, including law enforcement, in the event of an attack. A city's role, whether in providing direct defense or indirect support, varies depending on the relationship between private critical infrastructure providers and the government.

[19] FIRST. http://www.first.org/

➜ **Test incident response capabilities and processes.** In the same way that cities test their capacity to handle major catastrophes, such as hurricanes and terrorist activity, they should plan to test those processes created to communicate, collaborate, and restore services in the event of a cyberincident. Response capabilities should also be routinely evaluated against the current cyberthreat landscape.

When integrated into existing response procedures run by fire and police departments, these efforts become more effective and are better managed and scaled. A cybersecurity strategy should include specific expectations for the private sector and for other government entities. Exercises, involving both municipal and private sector actors, help stakeholders understand their roles during a crisis and can better prepare them for responding to incidents.

More information on building incident response capabilities

- Forum of Incident Response and Security Teams: www.first.org
- NIST Computer Security Incident Handling Guide: http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

6 Boost public awareness, education, and workforce training

A vast number of online security incidents are caused by the unintentional actions of employees or citizens. It can take just one person to click an infected link, open an email message from a supposedly trustworthy source, or insert an infected USB drive into a computer to put an entire network of systems and information at risk. Cities can offer employees and citizens tools and best practices to not only help protect city assets but also to save money in cybercrime enforcement and cleanup. Training and education should occupy a central place in the approach to improving cybersecurity.

Recommendations

→ **Develop public awareness campaigns.** The strategy should identify an agency or entity responsible for raising public awareness of online risks and the need for cybersecurity. The City of Boston[20] sponsors one such campaign that raises awareness of cybersecurity, encouraging citizens to take a cyberpledge that includes education about browser safety and device security measures, along with advice on when and where it is safe to share personal information online. As early as 1999, the European Commission ran the Safer Internet Programme, which led to Safer Internet Day, an annual event that highlights the importance of online safety and security, now in 100 countries.

School districts can play an important role in educating young people about online security and smart online behavior. StaySafeOnline.org breaks cybersafety into simple steps and provides lesson plans, activities, and exercises for all grade levels.

Some older citizens may be more vulnerable to online threats because they have less experience using the Internet. Pop-up browser windows may trick seniors into downloading infected software, and email phishing scams may entice them to give away personal and financial information to criminals. Cities can work with organizations targeted to seniors on ways to stay safe in cyberspace. One helpful public private partnership is the Miami and Microsoft program, eSeniors, which provides free computer training and reduced-price technology to seniors in Miami neighborhood senior centers.[21]

→ **Cultivate employee development and workforce training programs.** Cities often struggle to attract and retain a talented workforce because they can't offer salaries and benefits commensurate with private enterprise. Incentives, such as reduced college tuition and specialized training, can help bridge this gap.

Simple steps for computer protection

- Install antivirus software, and regularly update it.
- Install hardware/software, such as a firewall, to manage communication between and among networks.
- Have a cloud or offsite backup of important files.
- Require users to authenticate when signing in.
- Regularly install operating system patches.
- Protect mobile devices with PINs, and keep mobile operating systems and apps up to date.

More information on cybersecurity education and training

- Multi-State Information Sharing and Analysis Center (MS-ISAC) Local Government Cyber and Information Security Policies: msisac.cisecurity.org/resources/local-cyber-policies.cfm
- Stay Safe Online: www.staysafeonline.org
- InSafe's Safer Internet Day: www.saferinternet.org

[20] "Cyber Security." City of Boston. 2014. www.cityofboston.gov/oem/ReadyBoston/cybersecurity.asp

[21] "Microsoft, Miami Offer Seniors Free Computer Training, Customized PCs." October 29, 2007. www.microsoft.com/en-us/news/press/2007/oct07/10-29eseniorspr.aspx

7 Enable public, private, and academic cooperation

Collaborating with the private sector, other public sector entities, and academic institutions to research, identify, and respond to online threats must be a critical component of a city's cybersecurity strategy.

In cities where government-controlled private entities manage critical infrastructure, a city's cybersecurity strategy can formalize the creation of public/private partnerships. The "Good Practice Guide on Cooperative Models for Effective Public Private Partnerships (PPPs)," listed on the next page, offers 36 recommendations on how to build successful partnerships for resilient security.

For city-to-city collaboration, cities can look at the work of C40Cities Climate Leadership Group as a model. In 2005, megacities from around the world came together to reduce carbon emissions and to increase energy efficiency. Led by mayors and city leaders, C40 works closely with participating cities to address climate risks and their impact on a local and global level.

Recommendations

- **Take advantage of private sector resources.** Local companies generally participate in civic life with programs that range from loaned executives to specialized training. A cybersecurity strategy should recommend creating programs that tap private sector companies, particularly technology companies. A loaned executive program, in which private sector employees act as unpaid city employees, can fill specific cybersecurity needs within a city's ICT organization and can provide expertise and new perspectives. Cities can also work with private partners to help accelerate the development of new technology companies and jobs. For example, Microsoft has state-of-the-art Innovation Centers in more than 100 cities around the world, offering organizations access to valuable resources, experts, and tools for collaboration and skills development.
- **Partner with universities.** Cities can support cybersecurity research and training at local universities and subsequently benefit from the outcomes. Increasing the number of trained cybersecurity professionals within a region can help a city recruit and employ top-notch experts. Universities can also provide valuable research into threats and vulnerabilities within a city.
- **Sponsor events to connect the public and the private sector.** Events can range from large annual summits of international representatives to smaller, more regular meetings with startups to boost innovative thinking.
- **Promote law enforcement cooperation while protecting privacy and civil liberties.** Law enforcement agencies must come up with ways to work with responders around the world, despite different privacy values and different technology capabilities. A cybersecurity strategy should recommend that a single entity, likely within the existing police department, take responsibility for cybersecurity issues and that adequate training and resources be provided to this entity, with appropriate laws and oversight to ensure privacy and civil liberties are protected and respected.

→ **Create a culture of technology innovation.** An innovation culture propels organizations that thrive in the new economy. Cities can create environments that encourage innovation. For example, Tech City UK aims to help digital businesses in London grow and develop new ideas. It provides advice on everything from staff recruitment, accounts preparation, and compliance to negotiating leases, marketing, and raising investment. In February 2014, during the worst flooding in recorded UK history, various government agencies opened up government flood-level data for a day-long #floodhack, hosted by Tech City UK, allowing developers to create innovative solutions to weather-related disasters.

More information on public, private, and academic cooperation

- EU Agency for Network and Information Security's Good Practice Guide on Cooperative Models for Effective PPPs: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps
- C40Cities Climate Leadership Group: www.c40.org
- Microsoft Innovation Centers: www.microsoftinnovationcenters.com
- Tech City UK: www.techcityuk.com

Conclusion

Establishing a city strategy for cybersecurity is an important element in maintaining a city's security while mapping a path to future. By creating a structured approach, thinking holistically about threats and vulnerabilities, and deploying strong practices to detect, mitigate, and communicate threats, a city can protect its citizens and safeguard its resources. However, there will be barriers. Strained city budgets can limit planning and development. Risk-averse city managers may inhibit collaboration and innovation. Privacy concerns may constrain activities. By clearly articulating the return on investment—financial, security, and quality of life—a cybersecurity strategy can overcome these obstacles and become an integral part of a city's transformation.

Microsoft supports municipal efforts to develop cybersecurity strategies. With much of the world's population located in urban areas, cities are uniquely positioned to confront and manage cybersecurity concerns. Microsoft stands ready to help city leaders keep their communities, and the world, safe and protected.

Cybersecurity strategy checklist

1. Build a risk-based approach to cybersecurity

□ Develop a clear structure for assessing and managing risk.

□ Assess threats to the city's cybersecurity using threat modeling.

□ Document and review risk acceptance and exceptions.

□ Make citywide assessment and management of risk an ongoing process.

2. Set clear priorities

□ Educate city leaders to understand and support the principles and to manage priorities.

□ Consider resiliency.

□ Leverage procurement processes to reflect priorities and risks.

3. Define minimum ICT security baselines

□ Establish minimum security baselines.

□ Define clear roles and responsibilities for supporting a security baseline.

□ Establish a system for continuous security monitoring.

4. Share and coordinate threat and vulnerability information

□ Set expectations for sharing threat and vulnerability information.

□ Create a cross-city mechanism for sharing.

□ Run cyberdrills to test game plans.

□ Emphasize privacy and civil liberty protections in threat information-sharing.

□ Apply relevant national or international standards for information-sharing.

5. Build incident response capabilities

□ Create a Computer Emergency Response Team (CERT).

□ Create clear ownership.

□ Engage private sector and national resources.

□ Enable consistent incident classification.

□ Test incident response capabilities and processes.

6. Boost public awareness, education, and workforce training

□ Develop public awareness campaigns.

□ Cultivate employee development and workforce training programs.

7. Structure public, private, and academic cooperation

□ Take advantage of private sector resources.

□ Partner with universities.

□ Sponsor events to connect the public and the private sector.

□ Promote law enforcement cooperation while protecting privacy and civil liberties.

□ Create a culture of technology innovation.

Microsoft